ADVANCED HIGH PERFORMANCE S-BOX BASED AES ARCHITECTURE FOR SECURED COMMUNICATION IN VLSI SYSTEM

A SYNOPSIS

Submitted by

R. ANUSHA PADMAVATHY

(Reg. No. 201908270)

in partial fulfillment for the award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRONICS AND ELECTRICAL TECHNOLOGY

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL – 626 126

TAMIL NADU, INDIA

NOVEMBER 2024

1. INTRODUCTION

In the modern era of ubiquitous digital communication, the need for robust and efficient data encryption techniques has become paramount. One of the most widely adopted cryptographic standards is the Advanced Encryption Standard (AES), which has proven to be a reliable and secure algorithm for a wide range of applications. However, as the demands for faster data processing and higher levels of security continue to grow, there is a constant need to optimize the AES architecture for improved performance and security in Very Large-Scale Integration(VLSI) systems. Thus, the core of the AES algorithm lies in the Substitution Box(S-box) operation, which is critical for the algorithm's security. This architecture features an advanced S-box design that delivers improved resistance against side-channel attacks and other cryptanalysis techniques, without compromising the overall performance.

Basically, to achieve high performance, the architecture uses parallel processing, executing multiple AES rounds concurrently to leverage VLSI's inherent parallelism. Then the key expansion module efficiently generates round keys, minimizing overhead and ensuring smooth integration with encryption/decryption. In addition to the robust S-box, the architecture includes security enhancements like masking, randomization, and fault-tolerance to protect against side-channel and fault-injection attacks. The confusion-function in the cipher text of AES algorithm is carried out by S-Box. With the aid of Look up Tables(LUT), the S-Box transforms the input 8 bit data into 8 bit secret data. In general, as AES relies on LUT's, large count of memory cells are necessary. Meanwhile, the rigid architecture of S-Box makes the LUT's insecure for various cryptographic attacks. Therefore, in the proposed research work, for securing large data against multi-level attacks, the defined AES algorithm along with S-Box that involves different key pattern generation is employed. Moreover, the key lengths of AES algorithm is sufficient to safeguard the classified data, up to the secret level. However, in case of side channel attacks, the cipher text gets protected, but influences the implementation. Therefore, in this research work, a modified Blowfish algorithm is proposed for secure VLSI communication.

2. LITERATURE SURVEY

The VLSI circuits possess memory enabling the transmission of data and hence the security of circuits is a crucial factor. Moreover, these circuits are vulnerable to various failures which have to be rectified by encryption and decryption approaches. The VLSI circuits is totally customised and used in a variety of applications. In order to achieve the

goal of encrypted transmission, cryptography is a crucial step. Hence this section deals with the survey of advanced encryption and decryption for data security with its advantages as well as drawbacks.

Nadeem Iqbal et al [1] have recommended the new image encryption design for greater image security and morality through a connection of De-oxyribo Nucleic Acid (DNA) computing and random maps. Image encryption and decryption schemes have built-in capabilities to prevent data loss and noise attacks. Nevertheless, chaotic maps suffer from defects such as complete product distribution and not dispersing chaotic intervals.

Kwen-Siong Chonget al [2] have implemented Side-Channel-Attack (SCA) counter measures for async-logic Advanced Encryption Standard (AES) accelerator, a randomised delay line control, as well as data propagation control. A sync logic interface and async logic AES core are the two primary components of async logic AES accelerator. A flip flop is used for transporting, multiplexing and for latching the data, which is controlled by synchronizing the logic interface and is effectively a simple state machine. An async logic AES accelerators is attacked by combining several attacking hypothesis models. However, this is particularly critical for high-speed applications, as the random delays affect timing predictability.

Lein Harn et al [3] have presented an encrypted data aggregation that performs well for wireless sensor networks (WSNs) applications. To increase the opposition to traffic tracking and analysis. A network transmits data more effectively by using data aggregation. The system enables piggyback data transmission from all nearby sensors. Nonetheless, to encrypt different messages and onetime pad encryption requires a significant quantity of secret key that has to be established.

Meshrif Alruily et al [4] have introduced modern data transmission methods and asymmetric DNA encryption technology to reliably carry data. A reliability of asymmetric encryption is essential. These secure message transmission techniques include Polymerase Chain Reaction (PCR), One Time Pad (OTP), DNA chip technology, DNA fragmentation and bimolecular structure. This employs a single key for both encryption and decryption. Nevertheless, a key must be transferred between sender and receiver in a secure manner.

Jiakun Li et al [5] have discussed a 6CC-4CC dual field Point Multiplication (PM)method based on modifying the PM schedule and maximizing the use of Karatsuba multipliers. It performs well overall and has a long and significant route. Modern performance and more adaptability for Elliptic Curve Cryptography (ECC)designs are

features of the designed architectures. Nevertheless, it also has remarkable universality across other fields, thus, not all ECC applications use this approach.

MD Whaiduzzamanet al [6] have proposed the IoT and fog-integrated parts to monitor data records and compare them through the developed security scheme. Furthermore, it improves the identification, which offers higher assurance than the protocol in use at the time, as a result of the usage of a source of energy and a gated approach. However, it does not reduce the temporal complexity.

Pengzhou He et al [7] have suggested an Binary Ring-Learning-with-Error(BRLWE)based scheme on the hardware platform with very low-complexity with this point of view on FPGA. The system achieves effective key management and distribution for numerous users in addition to an effective security posture. Nonetheless, widespread adoption of the cloud is limited.

Yudi Zhanget al [8] have explained a reliable data transmission method using asymmetric DNA encryption technology. The employment of a block chain is centrally managed to reduce down on server procurement expenses while AES cryptography is used to modify each block series to strengthen the security of transaction data. This system is capable of performing the cryptographic modification of block chain technology. Nevertheless, it does not concession by the adversary because the adversary do not obtain the key.

Ijaz Khalid et al [9] have introduced animage encryption topology that makes use of isomorphic elliptic curves. This technique reveal that it is secure enough to withstand differential, brute force and entropy attacks. Nonetheless, image encryption system that already exist, the designed scheme has high temporal complexity.

Rami Amiri et al [10] have proposed an ECC on FPGA concurrent configurable cryptosystem to encrypt and decrypt a stream of data. The symmetric encryption lacks a non-repudiation service that pinpoint the source of an attack. Additionally, computation efficiency gets enhanced, and power consumption is decreased, making this method particularly suitable for use in on-board embedded devices. Nevertheless, cryptosystem depending on the applications security requirements.

Jun-Sheng et al [11] have presented an FPGA-based dual-hiding asynchronous-logic (async-logic) advanced encryption standard (AES) accelerator, which is highly resistant against Side-Channel Attacks (SCAs). The asynchronous logic and dual-hiding mechanisms strengthen encryption, helping the FPGA-based accelerator maintain data

confidentiality under advanced cryptographic attacks. Nevertheless, it does increase the use of logic gates and memory, potentially limiting the scalability of the design for large applications.

Kebotogetse et al [12] have performed the lightweight Concealed Based Security Scheme (CBSS) for secure transmission within the Advanced Metering Infrastructure(AMI). Moreover, it enhances the AMI algorithm uncertainty and greatly increases the effectiveness of attacks based on fault tolerant. However, it reduces the number of necessary traces while using minimum additional processing or plaintext.

Pietro Nannipieriet al [13] have proposed an Advanced Encryption Standard (AES) based crypto processor implementation, in embedded System-on-Chip (SoC) applications. The advanced features of the AES crypto processor provide high performance, making it suitable for applications requiring fast and secure data processing.AES provides strong encryption and is widely recognized for its security, making it a reliable choice for protecting sensitive data. Nevertheless, there is no efficient key management for AES security.

Anusha R et al [14] have proposed an efficient and secure Mutual authentication (MA) mechanism for Radio Frequency Identification (RFID)devices, using lightweight block ciphers (LBCs) on FPGA Platforms. It provide robust security for RFID devices, ensuring secure communication between the reader and the tag. FPGA platforms support parallel processing, allowing LBCs to operate quickly and efficiently. This ensures fast, real-time authentication, which is critical in applications where quick response times are needed, like access control and inventory management. Nevertheless, implementing a more complex encryption process with certain key generating tools is needed.

Weihang Tan et al [15] have proposed novel modular polynomial multiplier and demonstrated fast Finite Impulse Response (FIR) filter architecture for lattice-based cryptography. It greatly increases efficiency and ensures security, according to the analysis of performance and security. The design ensures full utilization of hardware resources, leading to better performance and efficiency. Nevertheless, it struggles to scale efficiently, impacting both performance and resource usage.

Oladipupo et al [16] have focused on improving the security of WSNs and the energy consumption of the sensors to ensure the longevity of their life span. This technique significantly improves the performance of elliptic curve point multiplication. This aids in enhancing hardware speed. The findings show that, in terms of the primary

refresh mechanism, it performs noticeably better than the existing rival schemes. Nevertheless, itrequire high logic resources on FPGA.

Khalid Javeed et al [17] have presented the highly efficient area-delay optimized elliptic curve cryptography processor. The correlation between adjacent cypher pixels is used by an adversary to deduce details about the plain image. This correlation must be reduced in any encryption method. This method are readily modified to encrypt uncompressed colour images even though it is intended to encrypt gray scale images only. Its strong security features, providing robust protection against various cryptographic attacks. Nevertheless, fault tolerance, making the processor more susceptible to errors due to noise, environmental changes, potentially impacting reliability in critical applications.

Sunil Kumar et al [18] have developed AES with compact and efficient S-box structure for lightweight cryptography. Different analyses are used to examine the security strength of the designed method, and the results reveal that it is secure enough to withstand differential, brute force, and entropy attacks. This method uses the Kobltiz method to turn points on an elliptic curve from plain pixcels. Nevertheless, compared to other image encryption systems that already exist, this model scheme requires a reasonable temporal complexity.

Irshad et al [19] have presenteda novel hybrid approach that integrates block chain with RFID data, Generative Adversarial Networks, and Elliptic Curve Diffie-Hellman cryptographic techniques. It detects fake or tampered data in the RFID system by identifying unusual patterns or inconsistencies. This mechanism prevents fraud and ensures that only authentic, verified data enters the block chain. Nonetheless, poor connectivity delay the system's efficiency, especially in distributed environments.

Alharbiet al [20] have implemented aDCryp-Unit design that uses hardware resources efficiently and optimized throughput for ECPM. It ensures efficient use of resources, reducing the overall power consumption and increasing the speed of cryptographic computations. Before the original data is delivered to the recipient, the attacker pretend to be the original sender and change it. Nevertheless, it is not as flexible or adaptable to other cryptographic algorithms or operation and more versatile cryptographic accelerator.

3. RESEARCH PROBLEM

Normally, for improving the security of confidential data, many different types of encryption algorithms are employed. The easy implementation, as well as the high speed of AES algorithm, makes it well suitable for small devices. Hence, many different

encryption techniques are employed for secured data communication. In conventional times, an asymmetric DNA encryption technology is employed and it employs a single key for both data encryption and decryption, but necessitates proper security for transferring the information amid the sender and the receiver. Further, an MCU is developed for WBSNs that incorporates VLSI circuit architecture, with the aim of attaining affordability. This technique involves a wireless encryption encoder, which produces uneven cryptography, so as to protect the confidential physical data, however it is impossible for the technique to decrypt the cypher text with the aid of public key. Similarly, an AES Encryption structure called Low-Power AES Data Encryption Architecture (LPADA) uses S-Box and a control technique for decreasing the power consumption of AES, however, it is necessary to maintain its functionality at a stable condition, at the time of voltage adjustment. Therefore, to overcome the above stated issues, a novel technique is employed in the proposed research.

4. OBJECTIVES

In order to overcome the above stated drawbacks, a novel technique is proposed in this research and the contributions of the defined research are mentioned below.

- To resist the overall efficiency of the AES algorithm, leading to faster encryption and decryption processes through a high-performance S-Box.
- To improve the low power consumption, which is essential for battery-operated devices and systems using VLSI implementations.
- To investigate various cryptographic attacks, including differential and linear cryptanalysis, side-channel attacks, and timing attacks by implementing Blowfish algorithm.
- To enable security testing, including formal verification methods, to ensure integrity and security through Modified Blowfish algorithm in the VLSI context.

5. PROPOSED METHODOLOGY

The proposed system work is executed in two stages, which is illustrated as follows,

- Implementation of Advanced Encryption Standard in Memory (AESIM) Efficient, High Performance S-box Based AES Encryption and Decryption Architecture on VLSI.
- Implementation of Multi-Level Attack with Dynamic S-Box Variable Key Pattern Generation for Key Cohort Using AES.

- Implementation of VLSI Secure Comm: Advancements in Blowfish Algorithm for Secure Data Transmission.

5.1 Implementation of An Advanced Encryption Standard in Memory (AESIM) Efficient, High Performance S box Based AES Encryption and Decryption Architecture on VLSI.

The Advanced AES is used to secure data stored in main memory by encrypting it to ensure data protection. For authentication and secure routing, a hybrid cryptographic approach combines AES with Elliptic Curve Cryptography (ECC): AES encrypts routing information, while ECC secures the public key. This combined use of AES and ECC provides a robust security mechanism and integrated into the memory, this method is called AESIM. In the proposed method, the AESIM technique supports key sizes from 128 to 256 bits. Encryption of each key is performed iteratively, processing one 128-bit block at a time within a set duration. Along the data path, four S-boxes handle word-level block processing. These S-boxes encrypt data, while key updates are managed separately, not directly within the core parallel to the block. Distinct software paths for encryption and decryption blocks are self-contained, with each accessing a sequence of round keys and a block, enabling the core to be hardwired specifically for either encryption or decryption.

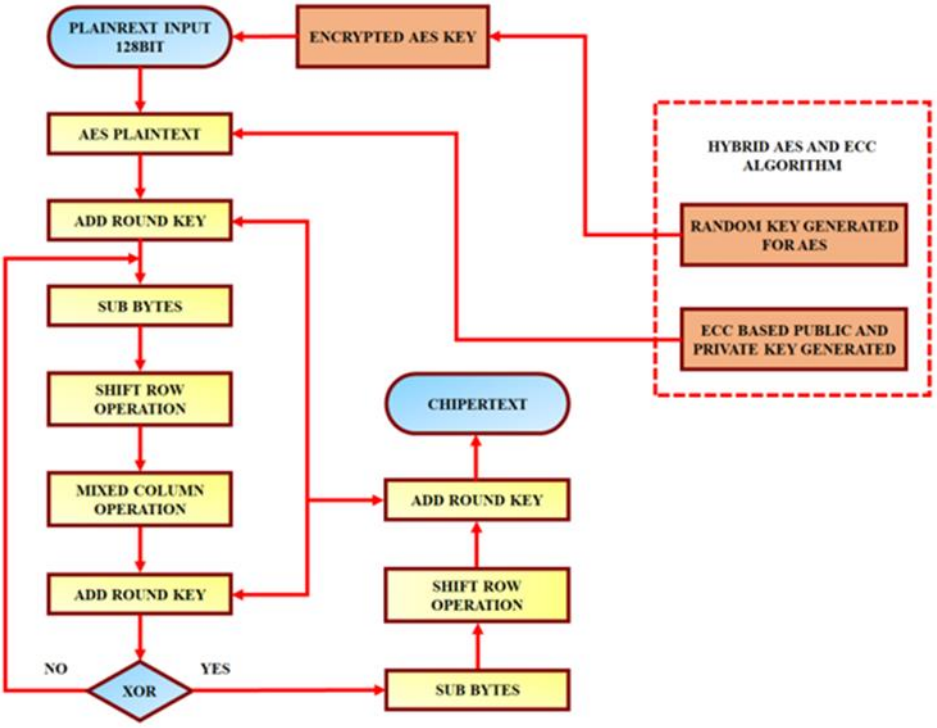

Figure 1 Overall Architecture of Work 1

This structure allows synthesis/build tools to optimize functionality and reduce size, ensuring that decryption remains unused, and the key remains operational as shown in Figure 1. The AESIM core excludes decryption for certain modes like counter mode (CTR), eliminating the need to process decryption blocks. Efficiency is further enhanced by using a single S-box or by expanding to 8 or even 16 S-boxes, this reduces the cycles per round to two rounds.

5.2 Implementation of Multi-Level Attack with Dynamic S-Box Variable Key Pattern Generation for Key Cohort Using AES.

In communication filed, privacy is the most vital issue, and many challenges are faced by the present communication field. Hence, many different types of encryption algorithms are employed for security purpose. In VLSI, it provides high security than the conventional techniques. In the proposed method, a variable key pattern which produces different key for each message is introduced, and it prevents multi-level data attacks.At the start, a key expansion component, a data encryption unit, and some basic control logics are integrated. A 128-bit plaintext is provided as an input and the encryption method is initiated by using a round key method.

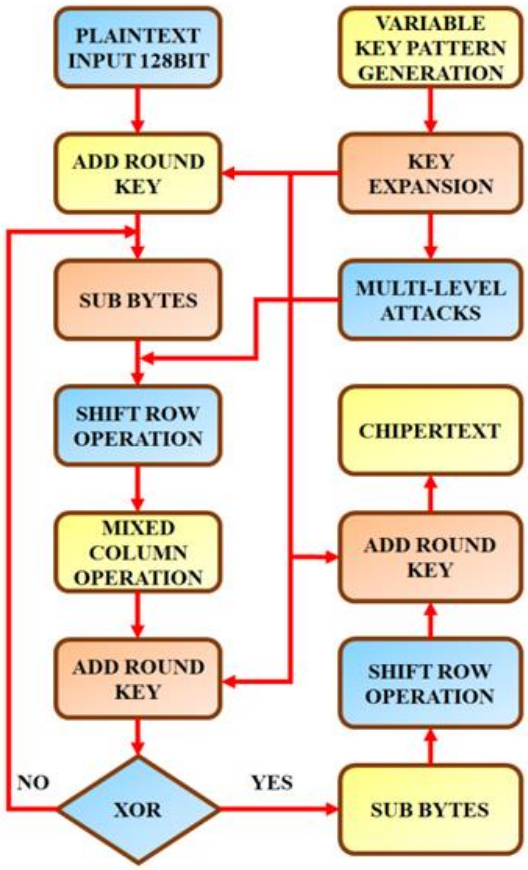

Figure 2 Overall Architecture of Work 2

Depending on AES method, a new key is generated at each round, such round key is 4x4 array of 128 bits as shown in Figure 2. It separates inputs into bytes and each byte using an S box during sub Bytes phases. Every cipher row is moved in a shift row. Every cipher column is moved correspondingly in the Mix column. Thus, input text is converted to cypher text and encrypted. Every process, including add round key, mixed column operations, or shift row procedure, is carried out in reverse for decryption. This work introduces variable key pattern production, which produce unique keys for each message to resist multiple attacks.

5.3 Implementation of VLSI Secure Comm: Advancements in Blowfish Algorithm for Secure Data Transmission.

The system processes a 64-bit plaintext block via a Key Expansion Unit, which generates round keys using the encryption key. A 16-round. Feistel structure, based on a modified Blowfish algorithm, handles the encryption/decryption process. Plaintext is split into two 32-bit halves (left and right) each round applies:

- A key-dependent substitution on the right half.
- XOR with the left half to produce a new right half.
- The original right half becomes the new left half.

After 16 rounds, the halves recombine into a 64-bit cipher text, ensuring secure communication. Algorithm modifications (e.g., S-boxes, key scheduling) enhance security and performance.

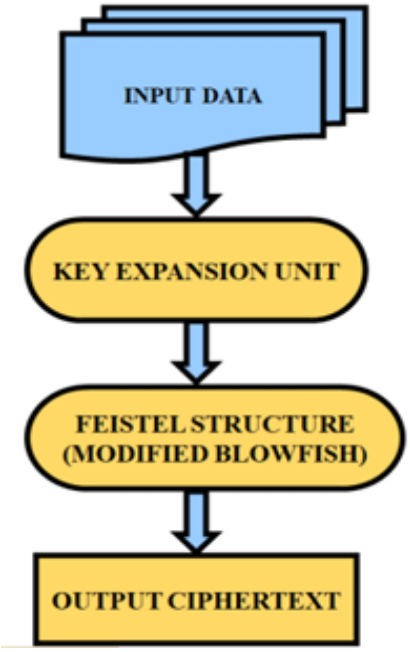

Figure 3 Overall Architecture of Work 3

These modifications are designed to improve the overall security and performance characteristics of the encryption/decryption process as shown in Figure 3. VLSI design ensures efficient hardware integration for high-speed data communication with robust encryption/decryption.

5.3.1 Modelling of Existing Blowfish Algorithm

The Blowfish (BF) algorithm is a symmetric-key block cipher widely used in encryption, including VLSI-based communication security systems. It operates on 64-bit plaintext blocks and supports variable-length keys ranging from 32 to 448 bits.

The algorithm consists of two main phases:

1) Key-Dependent S-Box Generation:

- Initializes four 32-bit S-boxes, each with 256 entries.
- Fills the S-boxes with a pseudorandom permutation of numbers 0 to 255, derived from the binary representation of the sine function.
- Modifies the S-boxes using the encryption key through a key scheduling algorithm to ensure key dependence.

2) 16-Round Feistel Network

- Splits the 64-bit plaintext into two 32-bit halves (left L and right R).
- Performs encryption/decryption through 16 rounds of substitution and permutation.

The variable-length key provides flexibility for different security needs, while the algorithm's high-speed performance makes it ideal for secure data encryption in high-performance applications.

5.3.2 Modelling of Encryption and Decryption Procedure

1) Decryption Procedure:

a) Key Expansion:

Initializes four 32-bit S-boxes (S_1, S_2, S_3, S_4),with a same fixed pseudo random permutation of numbers 0 to 255.

b) Plaintext Initialization:

Take 64 bit plaintext as input and two 32 bit halves, the left (L) and right (R) halves.

c) Feistel Network Rounds:

Perform 16 rounds of the Feistel network.

d) Cipher text Generation:

After the 16 rounds, recombine the final left (L) and right (R) halves to produce the 64 bit plaintext.

2) Decryption Procedure:

- The decryption process is same as encryption process, but the round keys are applied in reverse order.

a) Key Expansion:

Initializes four 32-bit S-boxes(S_1, S_2, S_3, S_4),with a same fixed pseudo random permutation of numbers 0 to 255.

b) Cipher text Initialization:

Take 64 bit plaintext as input and two 32 bit halves, the left (L) and right (R) halves.

c) Feistel Network Rounds:

Perform 16 rounds of the Feistel network, but in reverse order compared to encryption process.

d) Plaintext Recovery:

After the 16 rounds, recombine the final left (L) and right (R) halves to produce the 64 bit plaintext.

The Feistel network structure ensures identical encryption and decryption processes, differing only in the round key order. Key-dependent S-boxes and the F function provide the necessary confusion and diffusion, making the Blowfish algorithm secure and efficient for VLSI communication security applications.

5.3.3 Modelling of Modified Blowfish Algorithm

The MBF algorithm improves the security and performance of the original Blowfish cipher with these key changes:

a) Increased Key Length:

Extended from 448 bits to 512 bits for stronger encryption.

b) Improved S-Boxes:

Redesigned to resist modern cryptanalysis techniques.

c) Reduced Rounds:

Decreased from 16 to 12, boosting performance without major security loss.

d) Streamlined Key Schedule:

Optimized for faster key expansion and reduced overhead.

These modifications make MBF more secure, efficient, and suitable for modern cryptographic needs, while retaining Blowfish's core strengths.

5.3.4 Steps for Modified Blowfish Algorithm in VLSI-Based Secure Data Transmission

a) Key Generation:

The 448-bit secret key is generated and stored in the VLSI hardware module.

b) Data Partitioning:

The input data stream is partitioned into64-bit blocks.

c) Plaintext Input:

Each 64-bit plaintext block is fed to VLSI hardware module.

d) Plaintext De multiplexer:

The 64-bit plaintext is split 32-bithalves, L (left) and R (right).

e) 12-round Feistel Network:

The L and R halves are passed through the 12-round Feistel network structure, which includes the F-Function.

f) F-Function:

The F-Function operates on the 32-bit input by dividing it into four 8-bit quarters, accessing the S-boxes, and performing modular additions and XOR operations toproduce the 32-bit output.

g) Swap and XOR:

After the 12 rounds, the L and R halves are swapped and XORed to produce the final 64-bitciphertext.

h) Ciphertext Multiplexer:

The 64-bit ciphertext is combined and output from the VLSI hardware module.

i) Transmission:

The ciphertext blocks are transmitted over the secure communication channel.This F function is a key component of both encryption and decryption process of MBF algorithm, providing the nonlinear substitution and mixing of the data.

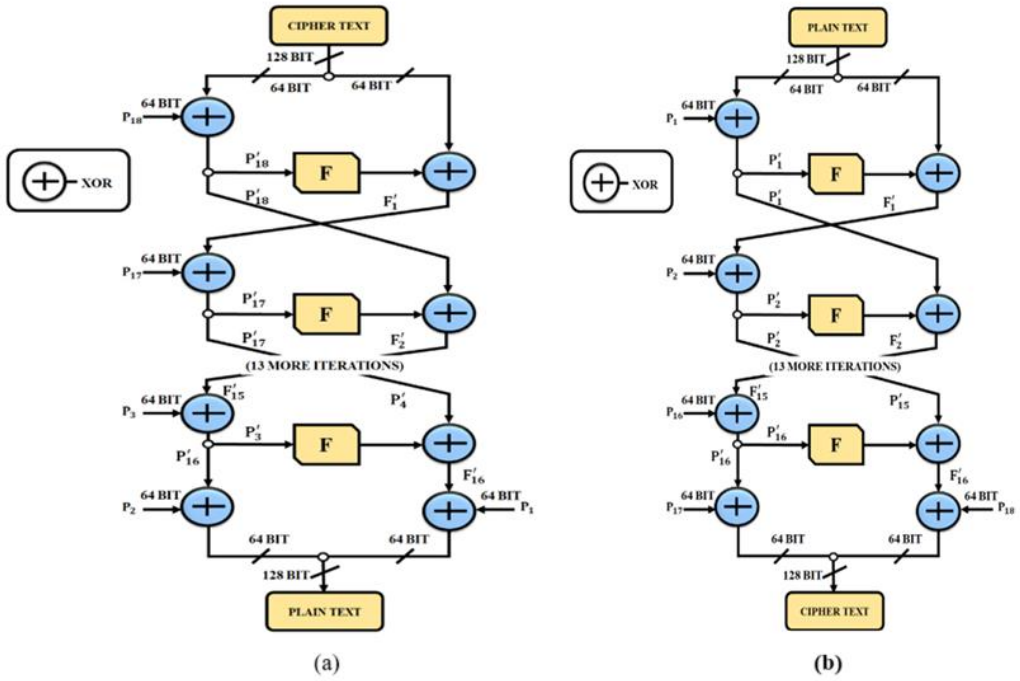

Figure 4 (a) Encryption and (b) Decryption Process

1) Encryption Process:

Initialization L and R with the 32 bit halves of plaintext block as shown in Figure 4 (a). For each of the 12 rounds:

- Compute F(R) using the F-Function.
- L=L XOR F(R)
- Swap L and R.
- Swap L and R one final time.
- L=L XOR P.
- R=R XOR P.
- The 64 bit cipher text is the combination of the final L and R.

2) Decryption Process:

Initialization L and R with the 64 bit cipher text block as shown in Figure 4 (b). For each of the 12 rounds:

- Swap L and R.
- Compute F(L) using the F-Function.
- R=R XOR F (L).
- Swap L and R one final time.
- R=R XOR P.

- L=L XOR P.
- The 64 bit cipher text is the combination of the final L and R.

The key aspects of Modified Blowfish implementation for secure data transmission include reduced rounds, a simplified key schedule, and an optimized F-Function. These enhancements enable a compact, efficient VLSI hardware module for secure, high-speed data transmission.

6. RESULTS AND DISCUSSION

In this research work data attacks in communication systems are rising due to VLSI improvements. To maintain confidentiality, this research introduces an AES algorithm-based Dynamic S-Box technique. This AES algorithm generates various keys from symmetrical keys using sub-keys, helping to restrict attacks. The technique is synchronized with encryption and decryption to ensure a secure and reliable AES algorithm. Initially, data encryption is performed using a cipher key, and during decryption, the encrypted data is decrypted using cipher text. The technique's significance is investigated using Xilinx software.

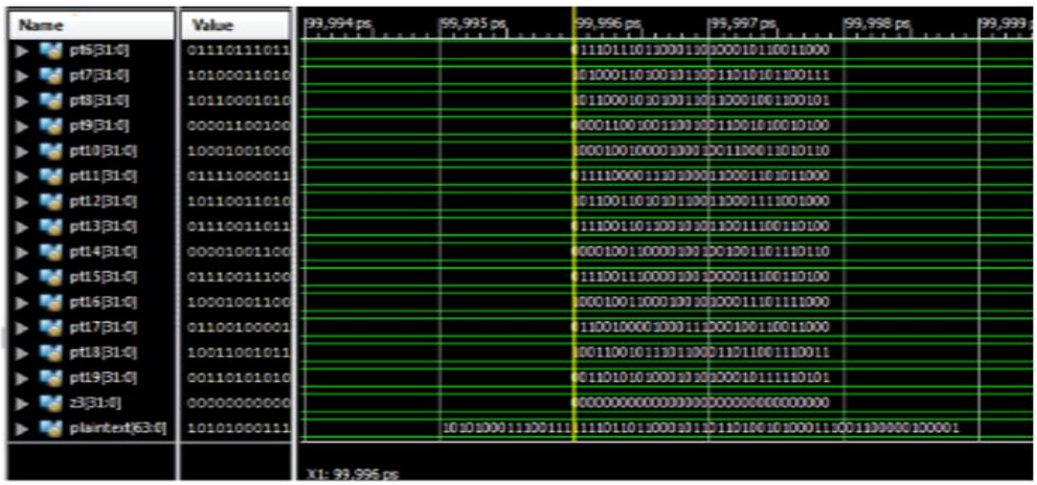

Figure 5 Encryption of plaintext

Figure 5 shows the plaintext encryption result. The plaintext, which is the original, unencrypted data, serves as the input to the proposed modified Blowfish encryption algorithm. This readable data, in the form of text or numbers, needs to be transmitted securely and protected from unauthorized access. It represents the sensitive information that must be safeguarded during transmission.

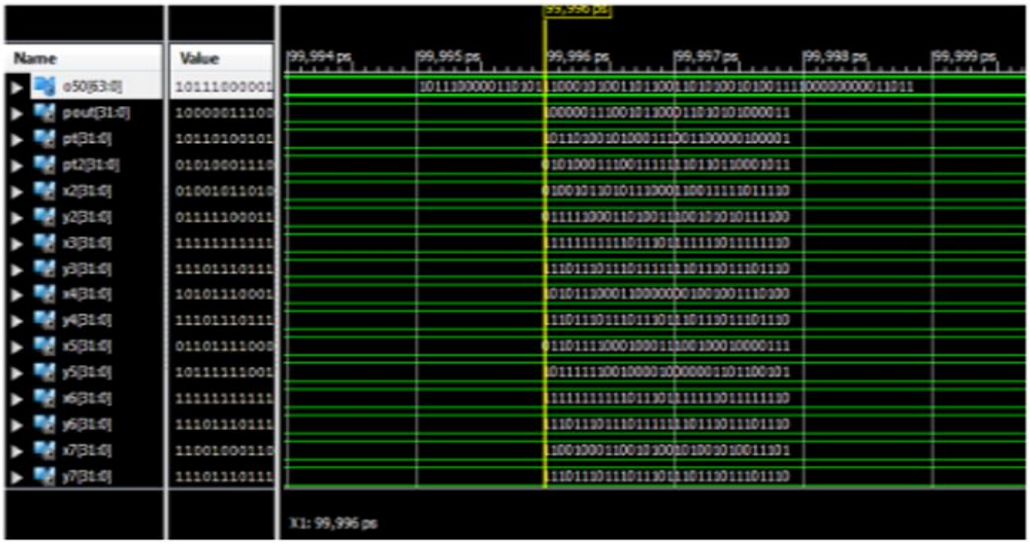

Figure 6 Encryption of Cipher text

Figure 6 illustrates the cipher text, the encrypted form of the original plaintext data generated by the modified blowfish algorithm. It is the output of encryption process and is transmitted securely over communication channel. The cipher text appears as random, unintelligible data that is nearly impossible to decrypt without the correct key. It serves as secure representation of sensitive information, effectively screening the original plaintext. The cipher text is the final result of the modified blowfish encryption process, sent over the secure communication link.

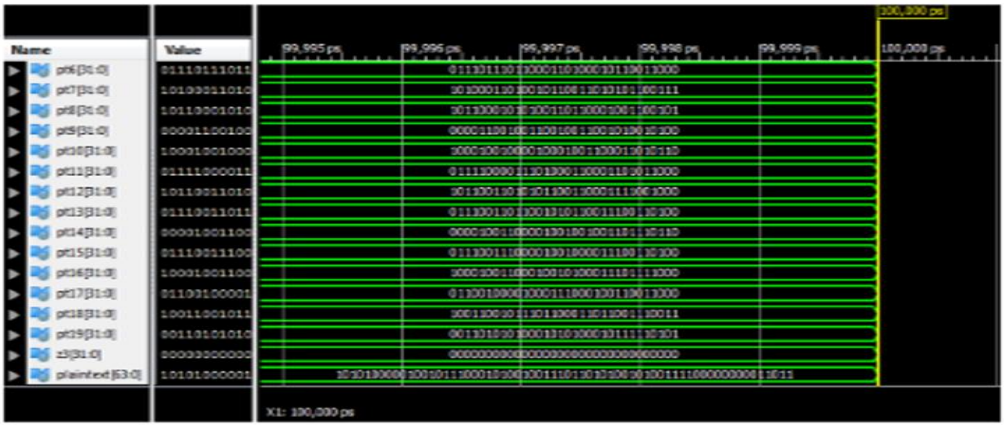

Figure 7 Decryption of Plaintext

Figure 7 shows the decryption process of the modified blowfish algorithm, which takes the ciphertext as input and uses the correct encryption key to recover the original plaintext. This plaintext is the readable intelligible version of the information is

secured during transmission. The decryption process reverses the complex transformations of encryption, restoring the original plaintext from the ciphertext. Accurate recovery of plaintext is crucial for the Blowfish algorithm's security and effectiveness in secure data transmission.

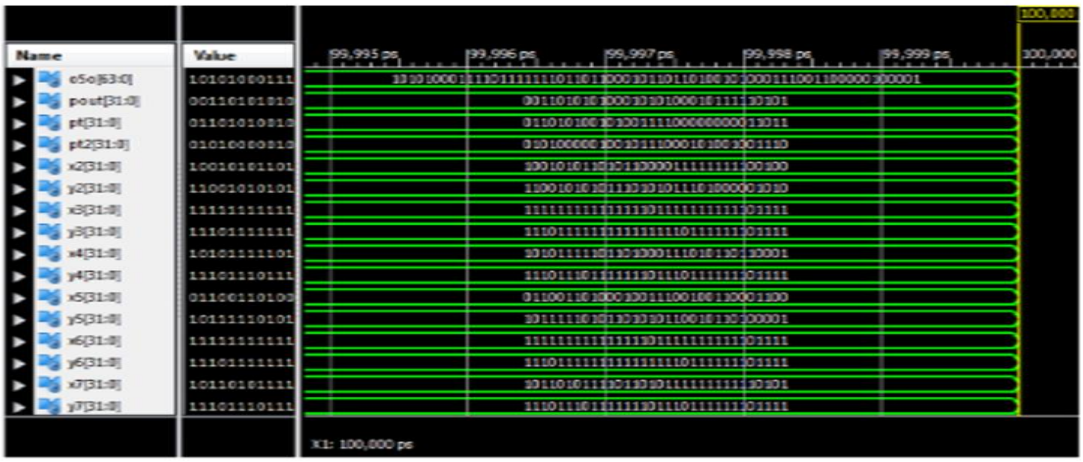

Figure 8 Decryption of Cipher text

Figure 8 shows the cipher text, the encrypted form of the original plaintext data used in the decryption process. This cipher text represents the secured, unreadable version of sensitive information transmitted over the communication channel. During decryption, the proposed blowfish algorithm uses the correct encryption key to reverse the encryption process, converting the cipher text back into the original plaintext. Maintaining the integrity of the cipher text is essential for successful decryption and retrieval of the protected information.

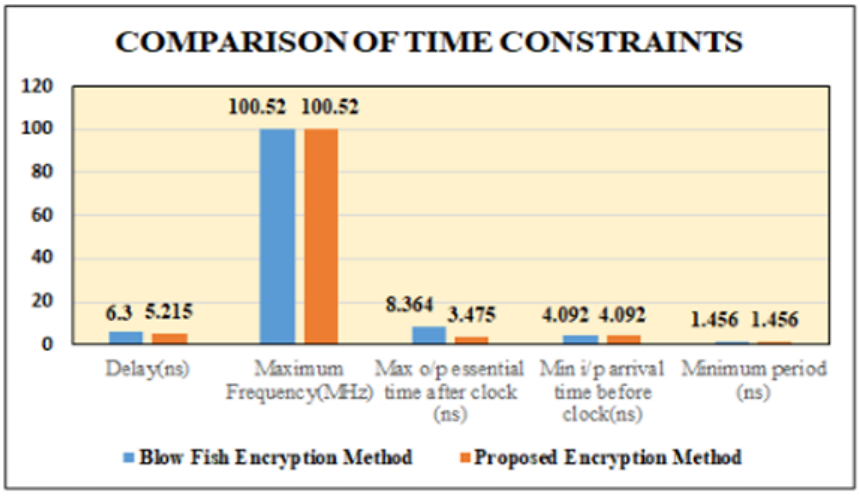

Figure 9 Comparison of time Constraints for Encryption process

Figure 9 compares the time constraints for the encryption process. The graph shows that the proposed modified blowfish algorithm achieves a shorter encryption duration compared to other topologies.

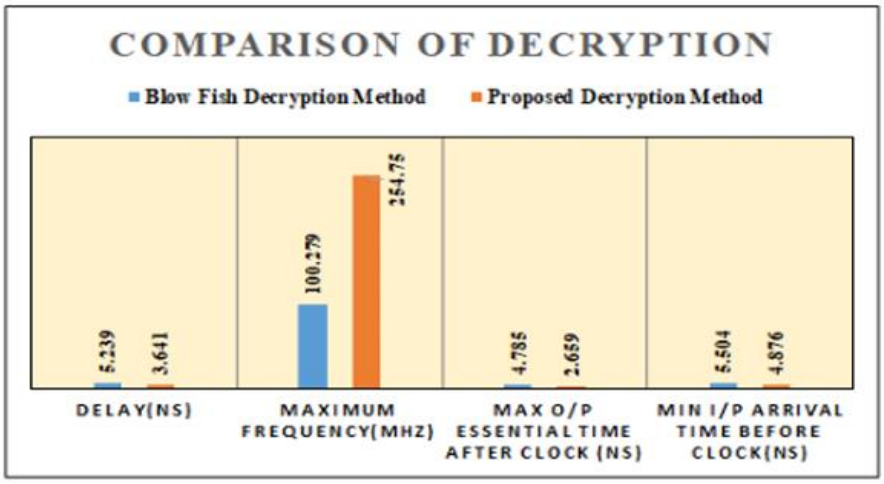

Figure 10 Time Constraints with Existing Decryption Method

Figure 10 illustrates the decryption process comparison for time constraints, showing that the modified blowfish algorithm of decryption process achieves better time constraints compared to others.

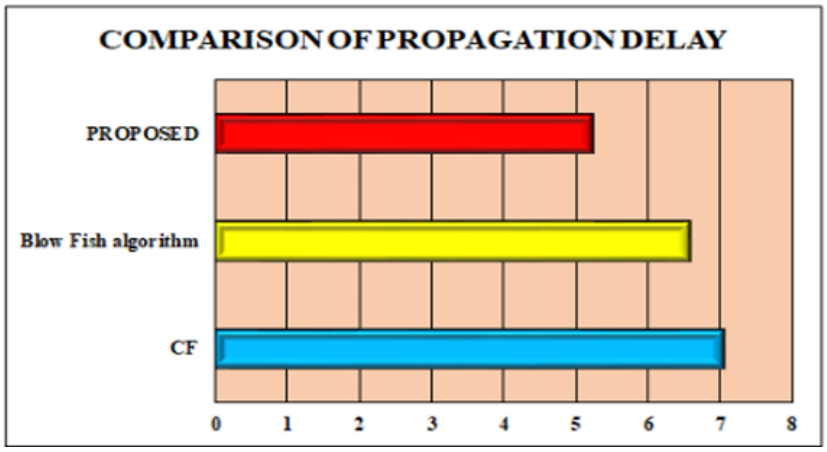

Figure 11 Comparison of Propagation Delay

Figure 11 compares the propagation delay for the conventional and proposed approaches, showing that the modified blowfish algorithm has less propagation delay compared to other topologies.

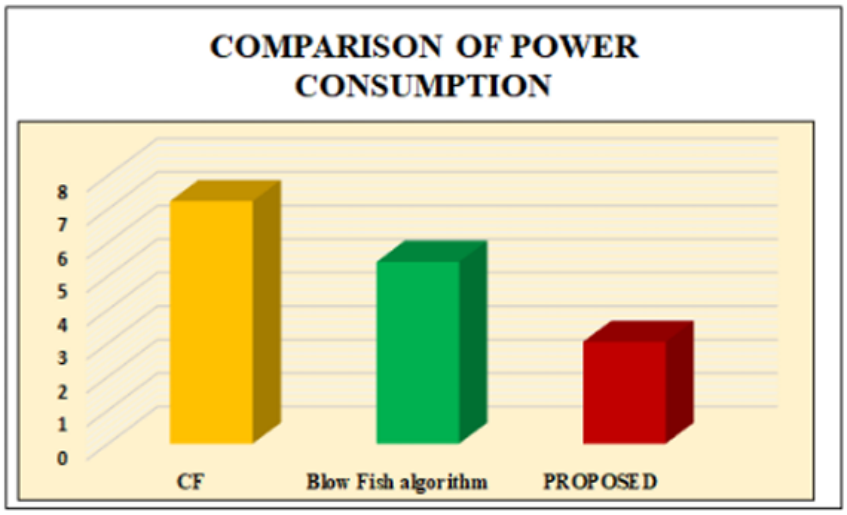

Figure 12 Power Consumption

The power consumption comparison is indicated in Figure 12, which analyzed that the modified Blowfish algorithm attains minimized power consumption compared to the other traditional approaches.

7. CONCLUSION

In data communication system, security systems, due to the improvements in emerging applications. While DES has become vulnerable, AES-based real-time memory encryption offers a secure solution, but performance and energy concerns demand more efficiency. By leveraging the inherent advantages of in-memory storage, such as high internal bandwidth and reduced data movement, AESIM overcomes the challenges associated with bandwidth-concentrated encryption methods. The efficiency of AESIM technique is evaluated based on various performance metrics for both encryption and decryption processes. In comparison to existing techniques, the proposed approach demonstrates remarkable results. AESIM leverages high bandwidth and minimal data movement, surpassing bandwidth limits of traditional methods. It achieves 0.735ns and 1.876ns encryption and decryption times, with minimal delay (2.641ns) and high frequencies (147.582MHz encryption, 215.450MHz decryption). Moreover, the minimum input and output time before and after encryption are 3.091ns and 0.674ns, respectively, while for decryption, they are 1.876ns and 0.669ns. Furthermore, for investigating the performance of the defined work, it is implemented in Xilinx Software. These results show AESIM’s efficiency, provides robust security for memory access in non-volatile systems

Then, this work presents an improved Blowfish algorithm for secure VLSI communication. While classic Blowfish balances security and performance, the revised version focuses on higher encoding speed, lower power consumption, and a smaller hardware footprint key factor for VLSI. Enhancements in key expansion and encryption boost throughput and efficiency. By leveraging parallel processing and optimized data paths, the improved algorithm outperforms traditional Blowfish. Simulations and hardware synthesis results demonstrate that the improved algorithm outperforms existing encryption standards in terms of speed and energy efficiency, making it ideal for real-time secure communications in resource-constrained VLSI environments.

9. ORGANIZATION OF THESIS

Chapter 1 Introduction: In this chapter, the basic details about communication systems and the use of AES in protecting the confidential data are discussed. In addition the different techniques that assists AES are also discussed in this chapter.

Chapter 2 Literature Survey: The information related to the existing topologies involved in communication systems are discussed. In addition, the different encryption and decryption techniques used in communicator system's are also discussed along with their pros and cons.

Chapter 3 Modelling of the System: This chapter includes the modelling of AES algorithm and the S-Box involved in protecting the data. Moreover, the key generation techniques used are also discussed in this chapter.

Chapter 4 Implementation of An Advanced Encryption Standard in Memory (AESIM) Efficient, High Performance S-box Based AES Encryption and Decryption Architecture on VLSI: In this chapter, the use of AESIM in protecting the confidential data from hackers are explained in detail. In addition, the results attained using AESIM are also discussed in this chapter.

Chapter 5 Implementation of Multi-Level Attack with Dynamic S-Box Variable Key Pattern Generation for Key Cohort Using AES: This chapter clearly discusses about the use of AES S-Box based data protection in VLSI system and it combines AES with ECC for both encryption and decryption. Moreover, the results attained using AES based S-Box technique is also deliberated in this chapter.

Chapter 6 Implementation of VLSI SecureComm: Advancements in Blowfish Algorithm for Secure Data Transmission: In this chapter, an improved Blowfish algorithm is employed for secured communication in VLSI systems. The proposed technique brings significant enhancements in encryption and decryption process. In addition, the results achieved with the aid of the defined technique is also discussed in this chapter.

Chapter 7 Results and Discussion: The overall results obtained from the proposed research work is deliberated in this chapter. Moreover, a comparative analysis is performed amid the proposed, as well as the conventional techniques, so as to foreshow the significance of the proposed work.

Chapter 8 Conclusion: The entire research work is concluded in this chapter and the suggestions, as well as the recommendations necessary for future works are also discussed in this chapter.

REFERENCES

1. Iqbal, Nadeem, Rizwan Ali Naqvi, Muhammad Atif, Muhammad Adnan Khan, Muhammad Hanif, Sagheer Abbas, and Dildar Hussain. "On the image encryption algorithm based on the chaotic system, dna encoding, and castle." IEEE Access **9** (2021): 118253-118270.
2. Chong, Kwen-Siong, Jun-Sheng Ng, Juncheng Chen, Ne Kyaw Zwa Lwin, Nay Aung Kyaw, Weng-Geng Ho, Joseph Chang, and Bah-Hwee Gwee. "Dual-hiding side-channel-attack resistant FPGA-based asynchronous-logic AES: Design, countermeasures and evaluation." IEEE Journal on Emerging and Selected Topics in Circuits and Systems **11,** (2) (2021): 343-356.
3. Harn, Lein, Ching-Fang Hsu, Zhe Xia, and Zhangqing He. "Lightweight aggregated data encryption for wireless sensor networks (WSNs)." IEEE Sensors Letters **5,** (4) (2021): 1-4.
4. Alruily, Meshrif, Osama R. Shahin, Hassan Al-Mahdi, and Ahmed I. Taloba. "Asymmetric DNA encryption and decryption technique for Arabic plaintext." Journal of Ambient Intelligence and Humanized Computing (2021): 1-17.
5. Li, Jiakun, Weijiang Wang, Jingqi Zhang, Yixuan Luo, and Shiwei Ren. "Innovative dual-binary-field architecture for point multiplication of elliptic curve cryptography." IEEE Access **9** (2021): 12405-12419.
6. Whaiduzzaman, Md, Md Julkar Nayeen Mahi, Alistair Barros, Md Ibrahim Khalil, Colin Fidge, and Rajkumar Buyya. "BFIM: Performance measurement of a blockchain based hierarchical tree layered fog-IoT microservice architecture." IEEE Access **9** (2021): 106655-106674.
7. He, Pengzhou, Ujjwal Guin, and Jiafeng Xie. "Novel low-complexity polynomial multiplication over hybrid fields for efficient implementation of binary ring-LWE post-quantum cryptography." IEEE Journal on Emerging and Selected Topics in Circuits and Systems **11**, (2) (2021): 383-394.
8. Zhang, Yudi, Zi Wang, Tatiana B. Kouznetsova, Ye Sha, Enhua Xu, Logan Shannahan, Muge Fermen-Coker, Yangju Lin, Chuanbing Tang, and Stephen L. Craig. "Distal conformational locks on ferrocene mechanophores guide reaction pathways for increased mechanochemical reactivity." Nature Chemistry **13,** (1) (2021): 56-62.

9. Khalid, Ijaz, Sajjad Shaukat Jamal, Tariq Shah, Dawood Shah, and Mohammad Mazyad Hazzazi. "A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes." IEEE Access **9** (2021): 77798-77810.
10. Amiri, Rami, and Omar Elkeelany. "FPGA design of elliptic curve cryptosystem (ECC) for isomorphic transformation and EC ElGamal encryption." IEEE Embedded Systems Letters **13,** (2) (2021): 65-68.
11. Ng, Jun-Sheng, Juncheng Chen, Kwen-Siong Chong, Joseph S. Chang, and Bah-Hwee Gwee. "A highly secure FPGA-based dual-hiding asynchronous-logic AES accelerator against side-channel attacks." IEEE Transactions on Very Large Scale Integration (VLSI) Systems **30,** (9) (2022): 1144-1157.
12. Kebotogetse, Otisitswe, Ravi Samikannu, and Abid Yahya. "A concealed based approach for secure transmission in advanced metering infrastructure." IEEE Access **10** (2022): 84809-84817.
13. Nannipieri, Pietro, Stefano Di Matteo, Luca Baldanzi, Luca Crocetti, Luca Zulberti, Sergio Saponara, and Luca Fanucci. "VLSI design of Advanced-Features AES CryptoProcessor in the framework of the European Processor Initiative." IEEE Transactions on Very Large Scale Integration (VLSI) Systems **30,** (2) (2021): 177-186.
14. Anusha, P., P. Raghavendra Rao, and N. Pratheksha Rai. "Secured authentication of RFID devices using lightweight block ciphers on FPGA platforms." IEEE Access (2023).
15. Tan, Weihang, Antian Wang, Xinmiao Zhang, Yingjie Lao, and Keshab K. Parhi. "High-speed VLSI architectures for modular polynomial multiplication via fast filtering and applications to lattice-based cryptography." IEEE Transactions on Computers **72,** (9) (2023): 2454-2466.
16. Oladipupo, Esau Taiwo, Oluwakemi Christiana Abikoye, Agbotiname Lucky Imoize, Joseph Bamidele Awotunde, Ting-Yi Chang, Cheng-Chi Lee, and Dinh-Thuan Do. "An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks." IEEE Access **11** (2023): 1306-1323.
17. Javeed, Khalid, Ali El-Moursy, and David Gregg. "EC-crypto: Highly efficient area-delay optimized elliptic curve cryptography processor." IEEE Access **11** (2023): 56649-56662.
18. Kumar, Sunil, Dilip Kumar, Hemraj Lamkuche, Vijay Shankar Sharma, Hend Khalid Alkahtani, Muna Elsadig, and Mariyam Aysha Bivi. "SHC: 8-bit Compact

and Efficient S-Box Structure for Lightweight Cryptography." IEEE Access (2024).

19. Irshad, Reyazur Rashid, Zakir Hussain, Ihtisham Hussain, Shahid Hussain, Ehtisham Asghar, Ibrahim M. Alwayle, Khaled M. Alalayah, Adil Yousif, and Awad Ali. "Enhancing Cloud-Based Inventory Management: A Hybrid Blockchain Approach With Generative Adversarial Network and Elliptic Curve Diffie Helman Techniques." IEEE Access **12** (2024): 25917-25932.
20. Alharbi, Adel R., Mohammad Mazyad Hazzazi, Sajjad Shaukat Jamal, Amer Aljaedi, Abdullah Aljuhni, and Dalal J. Alanazi. "DCryp-Unit: Crypto Hardware Accelerator Unit Design for Elliptic Curve Point Multiplication." IEEE Access (2024).

LIST OF PUBLICATIONS

1. R. Anusha Padmavathi, K. S. Dhanalakshmi : An Advanced Encryption Standard in Memory (AESIM) Efficient, High Performance S-box Based AES Encryption and Decryption Architecture on VLSI Wireless Personal Communications, **123**, (4).
2. Anusha Padmavathi Rajendran, Dhanalakshmi Krishnan Sadhasivam :Multi-Level Attack with Dynamic S-Box Variable Key Pattern Generation for Key Cohort Using AES The International Arab Journal of Information Technology (IAJIT), **20**, (5)
3. R. Anusha Padmavathi, K. S. Dhanalakshmi , K.Kalaiselvi, VLSI Secure communication: Advancements in Blowfish Algorithm for Secure Data Transmission, Conference: 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT).